

Federal Wireless Users' Forum Workshop
October 16, 2002

Background of the FWUF and Workshop Plan

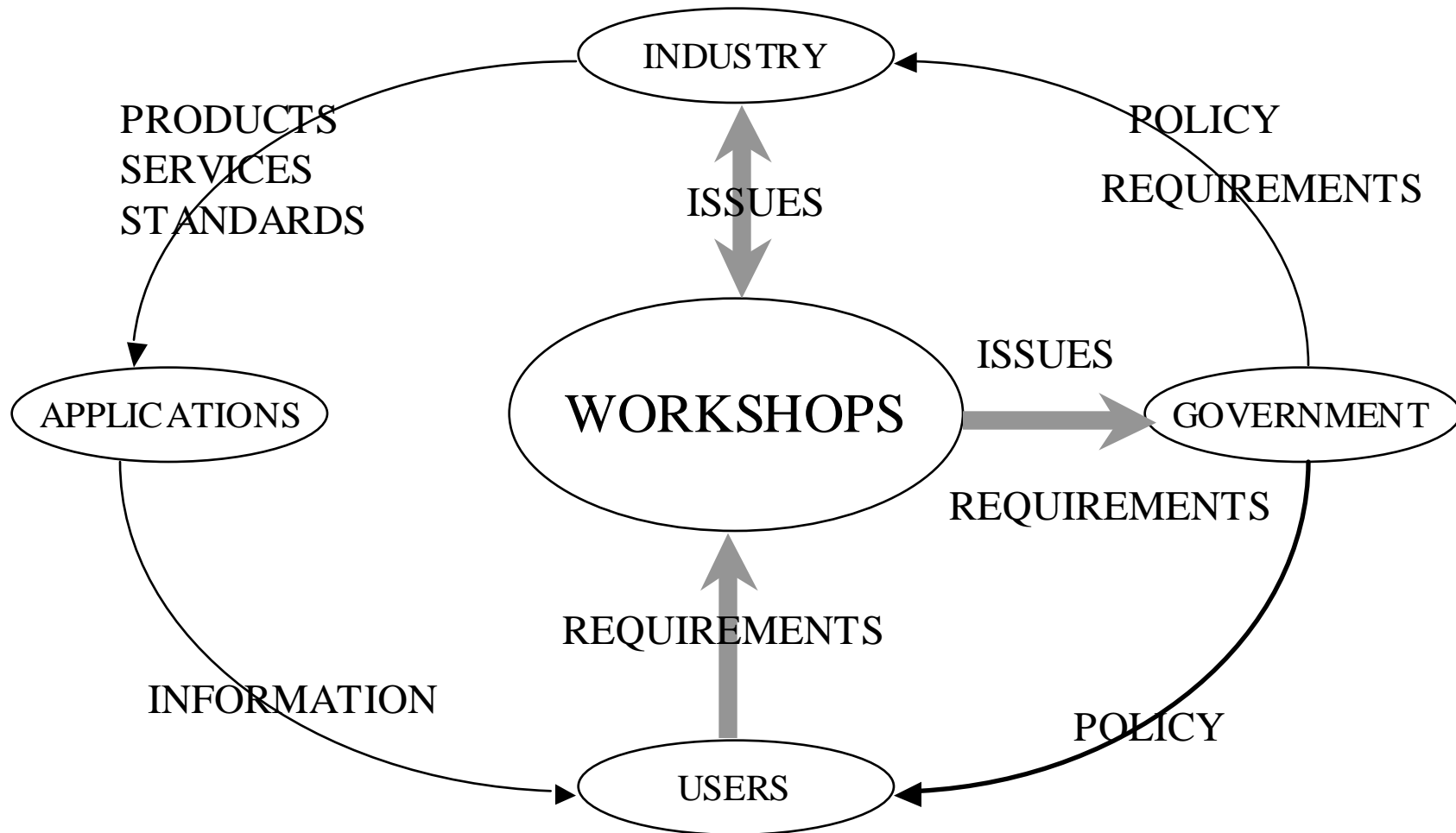
Mary K. Ruhl
National Security Agency
mkruhl@alpha.ncsc.mil

Federal Wireless Users' Forum

Objectives:

- Educate users about wireless communications
- Identify wireless telecommunications needs of government users;
- Facilitate information exchange
- Support the interoperability of emerging wireless services

How Workshops Work



Motivations

- Federal Government mandated to migrate from use of dedicated government frequencies to commercial leased systems
 - Moving to commercial, off-the-shelf equipment
 - Wireless services must accommodate the diverse national and international missions of the government
 - Concern over trends
 - fractured market/ technology wars
 - industry focus on near term problems
- ⇒ Need to provide clear definition of user requirements to support industry planning and standardization efforts

History of Federal Wireless Users' Forum

- NSTAC recommendations
- FWUF established in 1992 to provide user voice to wireless providers.
- FWPC established in 1993 to evaluate issues and provide recommendations on telecommunications policy.
- Identified broad, functional requirements for Federal wireless users
- Produced document, “Current and Future Functional Requirements for Federal Wireless Services in the United States” (August 1994)
- Basis for Federal Wireless Telecommunications Services contract

Federal Wireless Requirements

- FWPC document “Federal Functional Requirements for Commercial Wireless Services” (Revised May 1999 and December 2001)
- Broad array of needs for wireless products and services
- Much in common with the Business Community
- Scope covers:

Cellular	PCS	Mobile Satellite
SMR	WLAN	Paging
Wide Area Networks		WPBX
- Rapidly growing market
- Foresee most Government business conducted over wireless

Functional Requirements

- **D**igital
- **U**biquitous
- **I**nteroperable
- **T**ransparent
- **S**ecure

Federal Wireless Requirements

Priority Service

- Nationwide Service Access during Emergencies
- Uniform
- Standard terminal
- No Preemption
- Compatible with GETS/wired networks

Federal Wireless Requirements

Security

- Security is a “Must Have” requirement
- Three Tiers of Security
 - Commercial Products and Services
 - Security Enhanced Terminals (overlay)
 - Security Enhanced Infrastructure

Federal Wireless Requirements

Spectrum Issues

- New models for shared usage of spectrum
 - Use commercial services
 - Government as secondary user
 - Leased commercial service on Government frequencies
 - Government owned service and frequency
- Spectrum-flexible solutions for Military

May '02 FWUF Workshop

- Focused on changes in Federal wireless in the wake of 9/11 events
- Panel discussion on wireless lessons of 9/11
- Emerging commercial wireless services
- Interoperability issues and solutions
- Wireless Security
- Updates on Government Initiatives
- Discussion of user wireless requirements and issues

May '02 Workshop

Findings and Issues

- **9/11 underscore the critical need for wireless communications to be available and secure**
 - for national security and emergency response
 - Heightened awareness for the role of Government
 - Reported high degree of cooperation between response teams and commercial organizations
- **Effective interoperable communications require foresight, planning, coordination, and cooperation**
 - Training and drills essential
 - Current security environment calls for increased interoperability across all levels of government

May '02 Workshop

Findings and Issues

- **Progress has been on the deployment of WPS**
 - Greater Washington DC and New York City
 - Further support needed to ensure service across different technologies
- **Wireless security**
 - critical requirement
 - requirements for strong encryption, access control, authentication, data integrity, security management, wireless PKI
 - concern for malicious code to affect wireless devices
 - many agencies developing security policies for PEDs
 - more education on security, vulnerabilities, risks analysis, and risk management

May '02 Workshop

Findings and Issues

- **Diverse wireless applications**
 - PEDs, WLANs, CDPD, paging, mobile data networks, private radio, satellite
 - 3G shows great promise for interoperability and high-speed multimedia applications
- **Use different wireless services and technologies**
 - to support availability of communications during disaster response
 - Mobile devices are considered to be disposable
- **Wireless systems are now considered part of telecom infrastructure**
 - Must be integrated into national Homeland Security strategy

Workshop Objectives

- Learn about commercial wireless data services and mobile Internet
- Dialogue and seek input on:
 - wireless data technologies and services
 - products and service features for Federal users
- Partner with other users and industry
- Information sharing

Workshop Plan

Wednesday

- FWUF Keynote
- CTIA Keynotes
- “Brave New Government Panel”

Thursday

- Wireless Security Primer
- CTIA Keynotes and Exhibits

Friday

- Wireless Security, Interoperability, and Wireless Priority Service
- CTIA Keynotes
- Commercial Wireless Data Services and Technologies
- Dialogue Session on Wireless Data User Requirements and Issues
- Final Plenary

Future FWUF Events and Contacts

- Next workshop planned for April 8-10, New Orleans
- FWUF Web page *<http://www.nist.gov/fwuf>*
- Contacts

Technical

Jeng Mao, NTIA

jmao@ntia.doc.gov

Tim Havighurst, NSA

tjhavig@missi.ncsc.mil

Anna Entrichel, NSA

zalaboy@missi.ncsc.mil

Administrative

Donna Blanger

Booz Allen &

Hamilton

ph: (703)377-0699

[blanger_donna](mailto:blanger_donna@bah.com)

[@bah.com](mailto:blanger_donna@bah.com)